ITI Promoting Innovation Worldwide

December 6, 2021

Mr. Matthew Borman
Deputy Assistant Secretary for Export Administration
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

RE: ITI Comments Responding to Request for Comment Bureau of Industry and Security Interim Final Rule (IFR) BIS-2020-0038 pertaining to "Cybersecurity Items"

The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Most of ITI's members service a global technology market and service customers across all levels of government and the full range of global industry sectors, such as financial services, healthcare, and energy.

ITI's membership is comprised of 80 leading technology and innovation companies headquartered around the world from all corners of the information and communications technology (ICT) sector, including hardware, software, digital services, semiconductor, network equipment, and Internet companies, including providers of cybersecurity products and services. As a result, our industries have devoted significant resources, including expertise, initiative, and investment in cybersecurity and supply chain risk management efforts to create a more secure and resilient Internet ecosystem.
ITI appreciates the work and progress that has been made by the Bureau of Industry and Security (BIS), and the Department of State, in addressing the concerns raised by stakeholders over the proposed rule to control "intrusion software" in 2015. While the decision to renegotiate the underlying control with the Wassenaar Arrangement (WA) was not easy it has resulted in substantial improvements by tightening the scope of the rule to prevent the disruption of legitimate cybersecurity practices. Specifically, narrowing the scope of the technology control by excluding "vulnerability disclosure" and "cyber incident response," and excluding basic software updates from the control on "software" generation, command and control, or delivery of "intrusion software" go a long way in addressing the potential unintended consequences of implementing the WA's agreement on routine defensive cyber activities and related research.

Additionally, ITI and its members greatly appreciate BIS publishing an FAQ document to address some of the basic questions that are raised when attempting to assess the compliance obligations associated with navigating the complexities of the Interim Final Rule (IFR) and the new License Exception Authorized Cybersecurity Exports (ACE). A comprehensive FAQ document is a necessary and welcome tool, not only because it will help stakeholders navigate the technical complexity associated with analyzing which products or services may meet the definitions in the IFR, and the end use and end user

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

exclusions and exceptions in the ACE, but because it will particularly assist less well-resourced researchers and threat intelligence stakeholders who are important to the cybersecurity community and ICT ecosystem writ large.

ITI and its members are supportive of the administration's efforts to ensure that the products and services developed by innovators to secure the ICT ecosystem are not misused for malicious purposes and welcome the opportunity to provide ITI's views on the IFR. The below recommendations are intended to balance BIS' intent to adhere to the WA agreement with the needs of everyday cybersecurity practitioners. We look forward to working closely with you and would be pleased to discuss further any of the below recommendations. As the administration works to address comments submitted, further consultation with industry and technical experts is welcomed given the complexity of the underlining issues and the importance of the Rule.

General Comments

Cyber Information Sharing that is neither "vulnerability disclosure" or "incident response"

The definitions of "vulnerability disclosure" and "incident response" may be too limited to encompass the regular sharing of non-vulnerability and non-incident related cybersecurity information sharing, namely technical data on threat actors' tactics, tools, techniques, and behaviors, as well as certain vulnerability handling activities.

International standards (e.g. ISO/IEC 30111, 29147) recognize the process of vulnerability disclosure and handling, which includes the development, validation, and/or testing of a proposed remediation of the vulnerability. As such, information exchange or other actions often are necessary to facilitate the remediation and coordinate the mitigation and eventual public release of vulnerability details in a manner that best supports mitigation adoption by the ecosystem at large (public disclosure), which ultimately minimizes the risk that malicious actors learn of the vulnerability before a mitigation is available for network defense.

Moreover, it is common for security researchers, analysts, and other cyber practitioners to share technical information, including code, that may meet the definition of "technology" for the "development" of "intrusion software" unrelated to the remediation of a specific vulnerability or incident.

For instance, cybersecurity practitioners routinely share system artifacts that may or may not be related to an actual vulnerability or cybersecurity incident. It is the process of sharing and analyzing cyber-threat information and "Indicators of Compromise" broadly – characteristics of adversary behavior, preferred targets or methods of intrusion that can include exploit information or meta-analysis of the exploit – that are necessary to arm cybersecurity professionals with the knowledge necessary to make risk-based decisions about how to calibrate their defenses. These legitimate cybersecurity interactions may entail multiple sources of private information and regular interaction between members of the broader cybersecurity community.

Additionally, the global nature of cyber threats means that the License Exception ACE may not be an option to ensure regular information sharing activities can be easily conducted with researchers or

threat intelligence firms located in, or with employees from, Country Group E:1 or E:2, or Country Group D:1, D:2, D:3, D:4 or D:5 for "government end-users." The Middle East and Southeast Asia are areas of high malicious and criminal cyber activity in which valuable non-vulnerability and non-incident specific information is routinely shared to the benefit of U.S. entities cybersecurity posture.[1]

We appreciate that FAQ #15 broadly captures IT security roles and positions as eligible end users, as well as BIS' recognition of the importance of "rapid sharing" of cyber vulnerability and incident information in #17. However, additional clarity is necessary to ensure that the rule does not have the unintended consequence of chilling information sharing for U.S. companies attempting to gain insights from the global cybersecurity community. BIS indicates in FAQ #10, when discussing multinational companies, that it is not only the remediation of "cybersecurity incidents" that would qualify for the exclusion but also the "prevention" of an incident.

We recommend clarifying further the scope of "cybersecurity incidents" and "vulnerability disclosure" to include preventative, remediation development actions and other handling activities that may be considered "left of boom" in the FAQ document. Alternatively, adding a new qualified exclusion for cyber threat information from the control on "cybersecurity items" and License Exception ACE is needed to avoid creating a compliance barrier to rapidly sharing information that may be relevant to mitigating or preventing the compromise of U.S. entities.

We recommend additions be made to the FAQ document, to clarify that eligible end use spans the entire process of disclosing a vulnerability. The process of making a disclosure includes actions that extend beyond 'exchanging necessary information' and 'handling activities,' such as the development and testing of vulnerability remediation or other coordination activities related to effective response to a vulnerability. The reference to "conducting or coordinating remediation" (in the context of individuals or organizations responsible for "conducting or coordinating remediation") should be understood broadly to include all activities related to the handling of or response to the vulnerability or incident under international standards (such as ISO/IEC 30111, 29147) and other industry best practices. Moreover, we recommend adding PSIRTs (Product Security Incident Response teams) to the list in FAQ 15.

Favorable treatment cybersecurity end-user

In addition, ITI notes that regarding the application of ACE, certain exemptions are eligible for favorable treatment cybersecurity end users and certain restrictions are imposed on government end users. There are situations where the distinction between a favorable treatment cybersecurity end user and a government end user is not clear. In some circumstances a favorable treatment cybersecurity end user can also be a government end user. For example, in some countries, favorable treatment cybersecurity

[1] *See e.g.* Robert Falcone and Tom Lancaster, Emissary Panda Attacks Middle East Government SharePoint Servers, Unit 42 (May 28, 2019) available at https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/; Evolving Trends in Iranian Threat Actor Activity, Microsoft Threat Intelligence Center presentation at CyberWarCon 2021 on Nov. 16, 2021. available at https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/. ICS Joint Security Awareness Report (JSAR-12-241-01B), Shamoon/DistTrack Malware (Update B) issued Oct 16, 2012. available at https://us-cert.cisa.gov/ics/jsar/JSAR-12-241-01B.

end users, such as civil health and medical institutions, may provide public services and/or may receive funding from the government. A BIS clarification to address this type of overlapping situation is recommended.

Command and Control

Among the key changes made to address concerns from cybersecurity companies over the broad scope of the definition of "intrusion software" was adding the qualifier of "command and control" to the language related to hardware and software. ITI appreciates the work of the State Department and BIS to ensure that the control is focused on "use" of software and hardware, rather than the underlying technology. Ultimately, the success of this control in curbing human rights abuses or other malicious effects requires distinguishing legitimate business and security uses from criminal or other malicious uses. Such a distinction is not inherent in the underlying technology, but in the intents and purposes of the users, thus making technical features such as "command and control" potentially helpful objective distinguishing characteristics.

However, the IFR does not define "command and control." International standards bodies[2] and NIST[3] define "command and control" in terms of organizational decision making, rather than from the perspective of a computer security intrusion framework such as MITRE's ATT&CK matrix,[4] where the focus is on specific access to applications, data, and processes. These verified industry definitions in widespread use could create confusion when juxtaposed with the rule, thus undermining the intent to reduce the compliance burden and narrow the scope of the software and hardware controls. The FAQ document makes a number of references to the use of "command and control" as a technical characteristic of "intrusion software" making the logical inference that "command and control" means the capability to allow malicious access and communication to the "intrusion software." To ensure clarity BIS should add an entry to the FAQ document further defining the characteristics of "command and control" capabilities that will be covered under the "intrusion software" for the purposes of the EAR and solicit further comments on the matter.

Covered Products and Exploits

ITI companies also remain concerned over the specific categories of cybersecurity products covered by the control. FAQ #20 helpfully explains the distinction between tools with a passive analytical function, such as port or vulnerability scanning and packet sniffing, as outside the scope of the definition of "intrusion software" as they do not deliver an exploit. While FAQ #20 provides clarity for penetration testing toolsets, how will BIS handle non-public exploits?

---

[2] ISO 22320:2011, Requirements for Incident Response, prepared by Technical Committee ISO/TC 223, Societal Security. Available at https://www.iso.org/obp/ui/#iso:std:iso:22320:ed-2:v1:en.

[3] NIST SP800-59, NIST SP 800-60 Vol. 1-Vol.2 Rev. 1, (Issued Aug. 2003) by William C. Baker. Available at https://csrc.nist.gov/glossary/term/command_and_control

[4] Attack.mitre.org, *ATT&CK Matrix for Enterprise*. [online] [Accessed 6 December 2021].

FAQ #5 states that the WA agreement did not place exploits within the scope of ECCN 4D004, but the technology controls 4E001.a and 4E001.c would cover exploits not related to "vulnerability disclosure" or "cyber incident response." While FAQ #19 states that "information about the exploit is also not controlled when shared with the vendor" as it meets the definition of "vulnerability disclosure," this clarification does not cover sharing with others who are similarly situated but who aren't the vendor, such as the collaboration of researchers or of cybersecurity practitioners, who may have valuable information necessary to better understand the exploit itself or the threat actors that use it.

Similarly, FAQ #6 states that knowledge about an exploit can meet the definition of "technology" for the "development" of "intrusion software" leading to some confusion about the sharing of information about exploits, as well as the products that communicate exploit information. Cloud based endpoint detection and response products, or virtual security operation center (SOC) services may require a license under 4E001.a and 4E001.c. In those situations, the complexity of ACE - particularly its end use and end user restrictions and carveouts - will increase compliance burdens as companies and security researchers attempt to navigate which global entities with which they do business or share non-vulnerability, non-incident information are covered by the ACE.

We encourage BIS to consider a number of potential solutions to resolve this confusion and ensure that routine and legitimate research on exploits and threats can continue unimpeded. One possible solution is drafting an additional FAQ to ensure the rule captures the routine sharing of exploits for legitimate cybersecurity purposes. Alternatively, BIS could amend the applicable definition of "published" under §734.7 of the EAR to include communal cybersecurity research, clarifying that the sharing of exploit information for research purposes meets the definition of "fundamental research" under §734.7(a)(5)(ii) to ensure an existing exception from the EAR definitions of "technology" or "software."

"Reason to Know" Exclusion from the ACE

The rule adds a new License Exception ACE for "cybersecurity items" to avoid interfering "with legitimate cybersecurity research and incident response activities." The ACE exception, however, includes an end use limited to export of cybersecurity item to any end user if the exporter has "reason to know" the item will be used against a system without authorization. This standard of review implicates not just knowledge of a malicious use of the "cybersecurity item," but the broader "reason to know," creating uncertainty for the exporter, reexporter, or transferer. This is especially challenging given the dual-use capabilities of penetration or intrusion testing platforms.

Cybersecurity tool vendors may need to take active steps to ensure their products are used for their intended purposes. This is a regulatory and compliance burden that could inhibit the growth of certain cybersecurity startups or chill the sale of cyber products. Additionally, this determination becomes more complicated when considering the carve-out for "favorable treatment cybersecurity end users" in the D:1 and D:5 countries. How should exporters navigate the "reason to know" standard when it comes to exporting cybersecurity items to favorable treatment end users in countries with questionable human rights records and extensive government control over the private sector?

The "reason to know" standard injects uncertainty into the marketplace and may result in legitimate U.S. cybersecurity product and service providers from serving vulnerable global markets, weakening the global cybersecurity ecosystem. This uncertainty may also create a larger market for cybersecurity

providers in non-U.S. or WA countries. While there is no easy solution to this challenge ITI encourages BIS to consider expanding the limited definition of "favorable treatment cybersecurity end users." For example, educational institutions, essential services, and logistics providers do not qualify as "favorable treatment cybersecurity end users." Notably, the NotPetya ransomware attack hit several logistics providers, including the shipping company A.P. Moller-Maersk[5], and FedEx.[6] We recommend BIS consider how to increase the ability of U.S. firms to provide products and services to those industries, who are often targeted by threat actors, as doing so often has downstream benefits not only to U.S. companies in those industries but to the cybersecurity ecosystem writ large.

Compliance Costs

As has been discussed above, despite significant improvements BIS has made to ensure legitimate cybersecurity practices are excluded from burdensome licensing requirements, considerable ambiguity and complexity remain which will necessarily increase compliance costs, which will in turn sap resources from cybersecurity defense activities. The broad scope of "cybersecurity items" will likely generate significant financial burdens on a range of technology providers related to an array of legitimate security practices, despite the welcome availability of the ACE license exception, for at least two reasons. First, even with the benefit of the FAQ document some impacted stakeholders will still have difficulty interpreting when the requirements for some of the complex restrictions and exclusions apply, such as those related to "government end users" or "vulnerability disclosure" or "cyber incident response," respectively. It is assured that compliance costs for a wide array of industry and cybersecurity stakeholders will increase across the board as they devote resources to interpreting and applying the new rule. Second, the natural consequence for some compliance-driven exporters may be to assume a very conservative approach in their interpretations as to whether the ACE applies, potentially resulting in them "playing it safe" and applying for a greater volume of licenses. These compliance costs will be passed along to customers who are already struggling to dedicate the resources necessary to invest in, and maintain, an effective and resilient cybersecurity posture. BIS can mitigate some of these increased compliance costs by publishing decision trees that guide exporters through the parameters of License Exception ACE as well as the ECCNs introduced or affected by this rule.

Conclusion

ITI appreciates the opportunity to submit comments in response to this IFR. It is imperative that industry and government work together to achieve greater assurance that security products and services are being used to improve the resilience, security, and reliability of the global ICT ecosystem. We appreciate the work that has been done by BIS and the Department of State to ensure that technical experts and cybersecurity practitioners were represented during the WA deliberations and hope that precedent

[5] Andy Greenberg, *The Untold Story of NotPetya, the Most Devasting Cyberattack in History*, Wired (Aug 22, 2018) available at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[6] Kim S. Nash, Sara Castellanos, and Adam Janofsky, *One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs: FedEx says its expenses tied to malware attack was $400 million over past year, Merck put costs at $670 million In 2017*, WSJ (Jun 27, 2018). available at https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

continues going forward. Please consider ITI a resource on this issue, and do not hesitate to contact us with any questions regarding this submission.

Sincerely,

John S. Miller
Senior Vice President of Policy
and General Counsel

Mike Flynn
Senior Director, Government Affairs
and Counsel